解説

DNSのセキュリティ対策と運用状況の調査ツール

- DNSにおけるセキュリティ対策の現状 -

関谷 勇司 sekiya@sfc.wide.ad.jp
慶應義塾大学 政策・メディア研究科

石原 知洋 sho@sfc.wide.ad.jp
日本大学 理工学部物理学科

DNSは，インターネットにおける大規模分散データベースの成功例である．メール配信やウェブブラウジングといったインターネットの主要サービスは，DNSなしには考えられない設計となっている．つまり，DNSの保守はインターネットにおけるサービス基盤の保守である．しかしその一方で，DNSサーバの乗っ取りやなりすまし，DNSデータベースの不整合といった，DNSの運用を脅かす問題が発生している．そこで現在，DNSのセキュリティを向上させるためのいくつかの最新技術が開発され，実験されている．本稿では，現状のDNSが抱えるセキュリティ問題とその解決策に関して解説を行う．まず，DNSのセキュリティを脅かす代表的な攻撃について解説する．次に，その対策について，DNSのセキュリティを向上させるための新技術を交え解説する．さらに，新技術の導入を援助するDNS情報収集システムを提案し，その設計と実装について述べる．最後に，情報収集システムにて収集したデータの調査結果と分析結果を述べ，セキュリティの観点から見たこれからのDNS運用について解説する．

DNSの概要

DNSはDomain Name Systemの略である．DNSは，インターネットにおいて，主にドメイン名とIPアドレスの対応を管理する役目を担っている．IPアドレスを所有するホストの多くは，その名前とアドレスとの対応をDNSに登録する．これによって，インターネット上のどこからでも，ホスト名からIPアドレスを発見，もしくはその逆を行うことが可能となる．電子メールやウェブといったアプリケーションも，DNSなしには事実上運用不可能である．つまり，DNSはインターネットにおける各種サービスの基盤技術となっている．

また，DNSは大規模分散データベースとして設計され，構築されている．つまり，1つの大きなサーバで情報を集中管理する一極集中型のデータベースではなく，複数のDNSサーバが協調して動作することによって，1つのデータベースを形成している．これによって，耐障害性と規模性を確保している．したがって，ある1つのDNSサーバが不慮の事故によってサービスを停止したとしても，DNS全体としての機能は失われず，サービスを提供し続けることが可能である．

DNSのデータ空間は，ゾーンという単位によって管理される．また，**図-1**に示すとおり，ゾーンはその一部を他のゾーンとして分割し，管理権限を分割することができる．これを「ゾーンの委譲」という．ゾーンの委譲を繰り返すことにより，木構造のデータ空間が構成され，分散データベースが形成される．

DNSへの攻撃

前述の通り，DNSは，各種サービスの基盤技術となっている．そのため，DNSは健全に運用され，保守されるべきである．しかし，現状の運用は，すべてが健全であるとは言い難い．DNSサーバのなりすまし（Spoofing）や，DNSサーバの乗っ取り，さらにDNSサーバに対するサービス停止攻撃（DoS Attack）といった被害が多数報告されている．これらはCERT☆1発行の文章や，NANOG☆2にて行

われる議論の中に発見することができる．これらの代表的な攻撃の概要を述べる．

まず，DNSサーバの乗っ取りについて述べる．DNSサーバの乗っ取りは，DNSサーバのセキュリティホールを利用し，サーバの root 権限を搾取することによって行われる．DNSサーバを乗っ取ると，DNSのデータを自由に書き換え，偽の応答を行わせることが可能となる．また，乗っ取られたDNSサーバが管理する下位のドメインをも自由に書き換えることが可能となる．したがって，DNSサーバを乗っ取ることは，DNSサーバのなりすましを行うための最適な手段となり得る．

次に，DNSサーバのなりすましは，**図-2**に示す3種類の場合が存在する．(I) の場合は，リゾルバクライアントがDNSサーバに対して名前解決を要求した際に，第三者がソースアドレスを偽造したパケットを送信することによって，偽の回答を行う攻撃である．(II) の場合は，DNSサーバ同士の通信において，(I) の場合と同様に第三者によって偽の回答が行われる場合である．(III) の場合は，通信相手となるDNSサーバが乗っ取られており，データが偽造される場合である．どの場合も正しい名前解決を妨害し，攻撃者の意図通りに名前解決を偽造することが可能となる．

最後に，サービス停止攻撃について述べる．これは，無効な名前解決要求を特定のDNSサーバに意図的に大量に送信することで，DNSサーバの負荷を増大させ，通常のサービス提供を妨害する攻撃である．

攻撃への対策

DNSにおけるセキュリティ問題を解決するために，いくつかの新技術が考案され，実験されている．そこで本章では，DNSsec[1)]，TSIG[2)]，SIG (0) [3)]，TKEY[4)] という4つの新技術について解説し，それぞれの適用範囲と，セキュリティを向上させるための条件について述べる．

セキュリティ確保の新技術

本節では，DNSのセキュリティに関する新技術について解説する．

❑DNSsec

DNSsecは，公開鍵暗号方式を用いてデータ起源の認証を行う技術である．まず，あるゾーンに対して秘密鍵と公開鍵の鍵対を作成する．公開鍵はKEY RRにて配布する．そして，ゾーンに存在する各RR (Resource Record) に対して秘密鍵にて署名を行い，SIG RRに署名を記述する．したがって，各々のRRに対して，対応する SIG RRが少なくとも1つずつ存在することとなる．また，公開鍵と署名をRRとして公開することにより，既存のDNSの技術を利用して配布することが可能となっている．そして，名前を引くクライアントは，公開されている署名と公開鍵とを用いて認証を行い，データの起源を確認する．この際，配布されている公開鍵の正当性を保証するために，公開鍵自体もデータの起源が保証されている必要がある．すなわち，公開鍵自体が上位のゾーンの秘密鍵を使って署名されている必要がある．**図-3**に示すとおり，上位のゾーンから署名を連鎖させることによって，DNSの木構造全体のデータ起源を保証する．しかし，DNSsecは基本的にデータの起源の正当性を保証する技術であり，実際のトランザクションの正確性を保証する技術ではない．これを実現するには，TSIGやSIG (0) といった技術を併用する．

❑TSIG

TSIGは，秘密共有鍵を用いて，DNSサーバとクライアントとの間で行われるトランザクションを認証する技術である．サーバとクライアントにて秘密鍵を共有することで，あらかじめ認証されたクライアント以外からのサーバの利用を制限したり，メッセージの完全性の認証が可能となる．また，サーバ間でTSIGを適用することにより，ゾーン転送の認証やアクセス制限を行うことが可能となる．ただし，認証に秘密共有鍵を用いているため，あらかじめ信頼できる方法によって鍵を共有しておく必要がある．たとえば，フロッピーディスクなどを用いて鍵を交換する方法が挙げられる．この鍵交換を，ネットワークを通じて自動的に行う方法として，後述するTKEYという技術が存在する．

❑SIG (0)

SIG (0) もTSIGと同じく，DNSサーバとクライアント間，もしくはサーバ間のトランザクションの認証を提供する技術である．しかし，TSIGが秘密共有鍵を利用するのに対して，こちらは公開鍵暗号方式を採用している．SIG (0) RRによって配布される公開鍵を用いて，トランザクションの認証を行う．あらかじめ鍵を共有することなく，サーバクライアント間の通信における完全性が認証され

☆1 CERT Coordination Center (http://www.cert.org/)．
☆2 The North America Network Operator's Group (http://www.nanog.org/)．

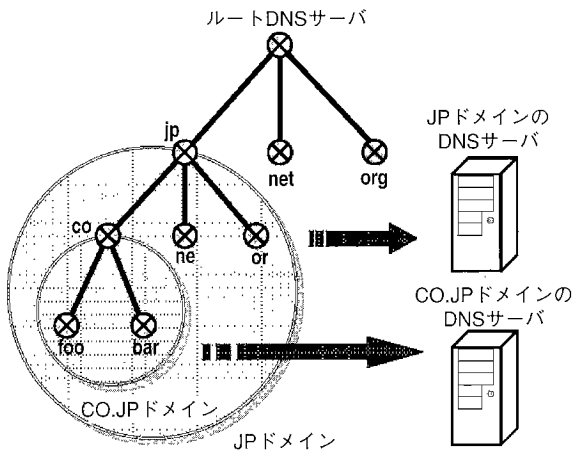


図-1　ゾーンの委譲

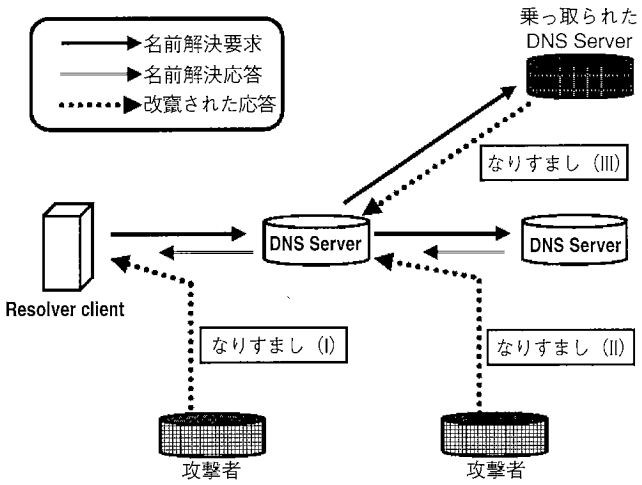


図-2　なりすまし攻撃

る．その一方，公開鍵暗号方式であるため，TSIG に比べて処理の負荷が増大する．

❑TKEY

TKEYは鍵の自動交換を行うための技術である．TSIG と併用して用いることで，DNSサーバとクライアントとの間で，秘密鍵を自動的に共有したり削除したりすることが可能となる．

新技術の導入

本節では，前章にて述べた，DNSサーバへの攻撃を防ぐための方法について述べる．

まず，DNSサーバの乗っ取りを防ぐ方法について述べる．これは，日頃からDNSサーバのセキュリティホールに関する情報に注意し，常に最新のDNSサーバを利用するよう運用努力を行うしか，基本的に防ぐ方法はない．しかし，もし乗っ取られた場合にも，DNSsecを用いてすべてのデータに対して署名がしてあれば，被害を最小限に食い止めることが可能である．データを改竄したとしても，正しい秘密鍵を用いて署名し直さない限り，正当性が保証されないからである．すなわち，運用上注意すべき点として，DNSsecの秘密鍵は，DNSサーバ以外のネットワークから切り放された外部記憶装置に保持しておくべきであり，ゾーンを署名する際は，ネットワークから切り放された安全な計算機にて行うべきだ，といえる．

次に，DNSサーバのなりすましを防ぐ方法について述べる．なりすまし (I) を防ぐには，DNSサーバとリゾルバクライアントの間にて，TSIGもしくはSIG (0) を利用する．これによって，偽の回答を判別することが可能となる．なりすまし (II) の場合は，DNSsecを用いることにより防ぐことが可能である．たとえDNSサーバのなりすましを行ったとしても，偽の回答の場合には，データ起源の認証に失敗するためである．なりすまし (III) の場合も，なりすまし (II) と同様にDNSsecが有用である．改竄したデータは，正しく署名されていないため，認証に失敗するからである．

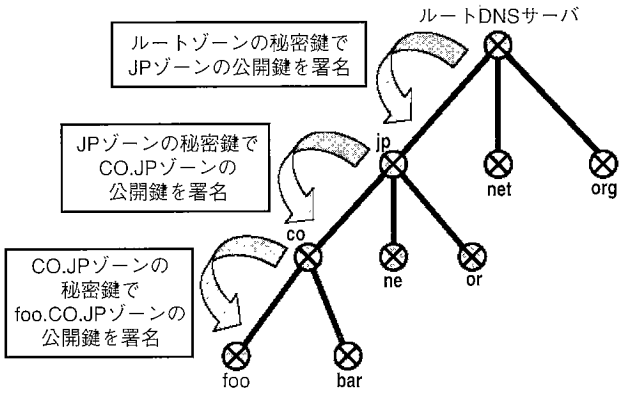
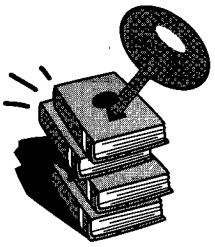


図-3　署名の連鎖

最後に，サービス停止攻撃の防御について述べる．サービス停止攻撃は，基本的に防ぐことが不可能である．DNSサーバに対しては，不特定多数のクライアントから名前解決要求メッセージが届くため，通常の名前解決要求なのか攻撃なのかを判定するのが難しいからである．最善の対処法は，DNSサーバでのメッセージのトランザクションを監視し，特定のクライアントから明らかに攻撃だと思われるトランザクションがある場合に，ルータにてフィルタを設定し防御することである．

以上述べたとおり，代表的な3つの攻撃のうちサービス停止攻撃を除く2つの攻撃は，新技術のDNSsecとTSIGを組み合わせることによって，防御もしくは被害を最小限に抑えることが可能である．



セキュリティ向上にむけて

DNS全体のセキュリティを向上させるためには，DNSsecやTSIGといった新技術の導入が有効であることが分かった．しかし，現状のDNSに対してDNSsecをそのまま導入することは困難であると考えられる．前述したとおり，DNSsecという技術は，上位のゾーンから署名を連鎖させることによってデータの起源を保証している．すなわち，DNSsecを有効に機能させるためには，ルートDNSサーバから末端のDNSサーバまで，ゾーン委譲が正しく行われている必要がある．しかし残念ながら，現状のDNSは必ずしも正確な委譲が行われているとは限らない．また，アップグレードされずに放置されている古いDNSサーバも，新技術導入の障害となる，したがって，DNSsecやTSIGといった新技術を効果的に導入するためには以下の前提条件が必須となる．

(1) DNSsecを有効に機能させるため，正確なゾーンの委譲を行う
(2) DNSサーバを最新のバージョンに保つ

DNS情報収集システム

DNS全体のセキュリティ向上を図るためには，前述した2つの前提条件を達成することが必要である．そして，これらの条件を達成するためには，管理ドメインを越えて現在のDNSの状況を的確に判断し，問題点を改善する必要がある．そこで，それらの条件を達成するための支援システムを，設計・実装した．本章は，その支援システムであるDNS情報収集システムの設計と実装について述べる．

情報収集システムの設計

本システムでは，前述した2つの前提条件を達成するために，以下の点を目標としてシステム設計を行った．

-DNS全体の委譲木の状態を監視する
-DNSのバージョン情報を監視する
-DNS管理者に対して，注意を促す

上記の目標を実現するためには，以下の情報が必要と考えられる．

-DNSの委譲木構造
-DNSサーバごとのIPアドレス
-DNSサーバごとのバージョン情報
-DNSサーバごとの，所有組織と管理者に関する情報

DNSの委譲木をルートDNSサーバからたどっていくことにより，委譲の正確性を確認することが可能となる．また，委譲木をたどっていく過程において発見された個々のDNSサーバに関して，IPアドレスや管理者情報，サーバのバージョン等の情報を収集する．

そこで，上記の情報を効果的に収集するためのシステムとして，**図-4**に示すDNS情報収集システムを設計した．このシステムは，次の4つのモジュールにて構成される．

1.DNSサーバ情報収集モジュール
2. 管理情報収集モジュール
3. 委譲確認モジュール
4. データベースモジュール

各モジュールの役割について説明する．

❑DNSサーバ情報収集モジュール

DNSの委譲木をルートDNSサーバからたどることによって，あるゾーンを管理するDNSサーバのFQDNとIPアドレス，委譲の有無，さらにDNSサーバのバージョンを調査するモジュールである．具体的には，ゾーン中のSOA (Start of Authority)，NSレコード，ゾーンを保持するDNSサーバのFQDNとIPアドレス，バージョン番号を記録する．そして，ゾーン中にて委譲が行われている場合には，委譲先も記録する．委譲があった場合には，委譲先のサーバにて同様なデータ収集を行う．これを再帰的に繰り返し，末端のDNSサーバまでの委譲情報を収集する．

❑管理情報収集モジュール

DNSサーバの所有組織と管理者に関する情報を収集するモジュールである．DNSサーバ情報収集モジュールにて収集した，ゾーンを保持するDNSサーバのFQDNとIPアドレス情報をもとに，RIRs☆3のwhoisデータベースに問合せを行い，情報を収集する．

❑委譲確認モジュール

DNS委譲の正確性を判定するモジュールである．上位のDNSサーバから委譲されているゾーンに関して，そのNS RRにあるDNSサーバが，本当に委譲先のゾーンの権威を持つサーバとなっているかを確認する．また，委譲元のNS RRに列挙されているDNSサーバと，委譲先のゾーン先頭に列挙されるDNSサーバが一致するかを確認する．

❑データベースモジュール

上記の3つのモジュール処理を経て生成された，各DNSサーバとゾーン，さらにゾーンの委譲に関するデータを格納するデータベースである．

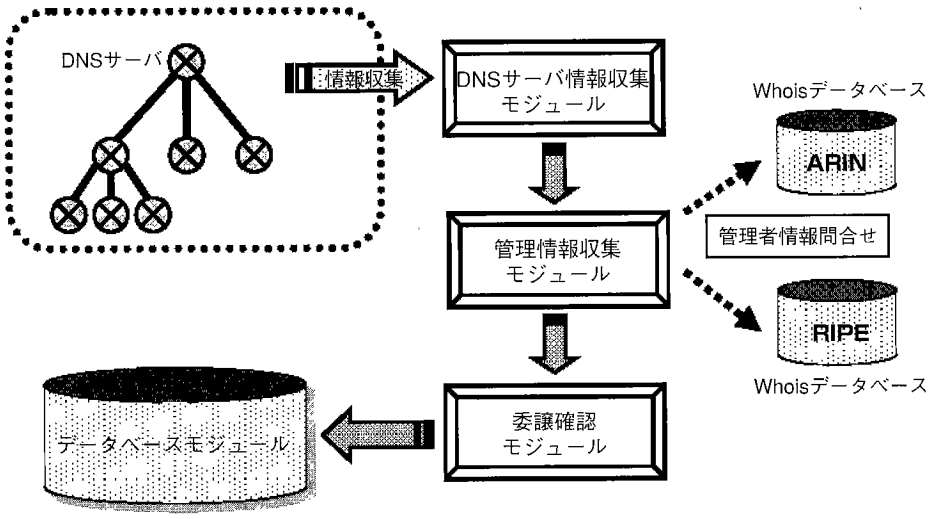


図-4　DNS情報収集システム

情報収集システムの実装

前述の設計に基づき，情報収集システムを実装した．情報収集システムの実装は，次に述べる環境にて行った．

-DNS - Sparc Station 20
-DNS - RedHat Linux 6.2（kernel-2.2.15）
-DNS - SCSI DISK 20G * 2

各モジュールの実装について述べる．

❑DNSサーバ情報収集モジュール

DNSサーバ情報収集モジュールは，perlにて作成した．DNSwalk☆4というソフトウェアに改造を加え，以下の情報のみを抜き出すよう作成した．

- ゾーンのSOA，MNAME，RNAME，NS，委譲の有無
-DNSサーバのFQDN，IPアドレス，バージョン番号

❑管理情報収集モジュール

本モジュールもperlにて作成した．DNSサーバ情報収集モジュールが集めたDNSサーバのIPアドレスをもとに，適切なInternet Registryのwhoisデータベースに問合せを行い，IPアドレスに対応する管理組織と管理者のデータを取得する．そして，DNSサーバ情報収集で得た情報と，whoisデータベースから取得した管理組織と管理者の情報をもとに，データベースモジュールに送るデータを作成する．

❑委譲確認モジュール

本モジュールもperlにて作成した．以下の2つの条件を満たす場合に，正確に委譲がなされていると判断するよう作成した．

(1) 委譲先のDNSサーバに対して問合せを出し，権威付き回答（Authoritative Answer）が返答される
(2) 委譲元のNSレコードに列挙されているDNSサーバと，委譲先のゾーン先頭にあるNSレコードに列挙されているDNSサーバが一致する

❑データベースモジュール

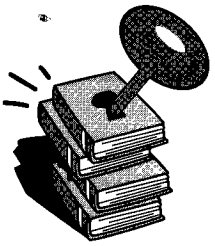
データベースモジュールは，rwhois[5]サーバに改造を加えて作成した．データベースサーバとしてrwhoisサーバを選択した理由は，次の2点である．1点は，普遍性である．通常のrwhoisもしくはwhoisクライアントを用いて情報検索が行えるという利点がある．もう1点は，拡張性である．本システムを分散して設置する場合，rwhoisプロトコルにて規定されている「Referral（参照）」という仕様により，容易にデータの分散を行うことが可能だからである．

以上の4つのモジュールを組み合わせ，DNS情報収集システムを構築した．

情報の分析

DNSセキュリティ向上のための2つの前提条件の実現を支援するため，DNS情報収集システムを構築した．そこで，本章ではこのシステムを実際に稼働し，収集したデータをもとに，DNSセキュリティ対策の現状について解説する．

☆3 Regional Internet Registriesの略．主にAPAN, ARIN, RPIEを示す．
☆4 bind配布パッケージのcontribに含まれる（ftp://ftp.isc.org//isc/bind/src/8.2.2-P5/bind-contrib.tar.gz）．



DNS情報収集システムの運用

本稿で述べたDNS情報収集システムを用いて，DNSの情報収集を行った．今回は，逆引きゾーンである，in-addr.arpaゾーンならびにip6.intゾーンに対して，本システムを実行した．その結果，逆引き委譲木を走査しデータを生成するのに，約6週間を要した．データ容量は，約5GBほどとなった．なお，今回示す調査結果は，2000年の4月に行われたものであり，ISI☆5という組織に位置するホストから行った．

なお，アドレスによってゾーン転送を制限しているDNSサーバからは，ゾーンのデータを収集することができない．したがって，そのDNSサーバが，逆引き委譲木の上位に位置している場合には，そこから下位の委譲を把握することが不可能となってしまう．そこで，ゾーン転送を制限しているDNSサーバのうち，委譲木の把握上重要と思われるDNSサーバに関しては，管理者に対して協力要請のメールを送ることによって，できる限り解決した．したがって，今回の調査では逆引きゾーンすべてを完全に走査することはできていない．また，バージョン番号の取得に関しても，取得に成功したサーバについてのみ結果を示した．しかし，DNSの現状を把握するにあたって十分と思われるデータ量は取得できたと考える．なお，本システムはhttp://www.isi.edu/~sekiya/rwhois/ にて試験運用されている．

統計情報から見るDNSの現状

まず，委譲に関する結果を，**図-5**に示す．走査した全183476委譲点のうち，約5.6%にあたる10322委譲点が，正常に委譲されていないという結果が出た．5.6%という数値は，意外に低いと思われるかもしれない．しかし，これはIPアドレスという限りある資源に基づいて形成される，逆引き委譲木に対して行った場合の結果であることを考えると，一概に低い数値だということはできない．さらに，委譲木が完全に壊れていた場合，それより先に委譲木を走査することができないため，その先の委譲がどの程度正確に行われているかを把握することは難しい．そして，同様の調査を，ドメイン名というほぼ無限の空間に基づいて形成されている正引き委譲木に対して行った場合，さらに高い数値が出ると考えられる．

次に，DNSサーバのバージョン番号に関する統計を，**図-6**に示す．さまざまなバージョンのDNSサーバが，現在稼働されていることが分かる．図中で網掛けになっている部分は，セキュリティホールの発見されているDNSサーバである．bind-8.2.2-P3以下や，bind-4.9.6以下は，有名ないくつかのセキュリティホールが発見されており[6]，これを悪用された場合，DNSサーバのサービス停止や，最悪の場合DNSサーバのルート権限を搾取される可能性がある．また，本調査で発見されたbindに関して，安全なバージョンと危険なバージョンの割合をまとめたグラフを，**図-7**に示す．危険なバージョンのまま運用されているbindが69%にものぼることが分かる．アップグレードされないまま放置され，運用されているDNSサーバが多いことがうかがえる．これらのbindは，早急にアップグレードされるべきである．

セキュリティ向上のための2つの前提条件に関して，その現状を把握するためのデータを示した．データから考えると，現状の委譲状態では，一部の委譲木においてDNSsecを有効に機能させることが困難だと考えられる．したがって，DNSsecを有効に導入するためには，本システムによって発見された不正確な委譲点を抜き出し，管理者に対して改善するよう注意を促す必要がある．また，DNSサーバのバージョン番号に関しても，危険なDNSサーバは早急にアップグレードする必要がある．危険なDNSサーバの管理者に対しても，注意を促すことが必要である．

以上より，現状のDNSにおいては，新技術を適用する土台が整っておらず，仮に新技術をそのまま適用したとしても，本来の効果を期待することはできないと考えられる．

これからのDNS運用

本稿では，DNSのセキュリティ問題について述べ，その解決策となる新技術について解説した．さらに，新技術を導入するにあたっての注意点について述べ，導入を支援するシステムを紹介した．その結果，新技術の導入はセキュリティ向上のために有効であることが分かった．しかし，有効に導入するためにはいくつかの前提条件が必要であり，現状のDNSがそれらの条件を必ずしも満たしていないことも明らかとなった．すなわち，新技術導

☆5 Information Sciences Institute（http://www.isi.edu/）．

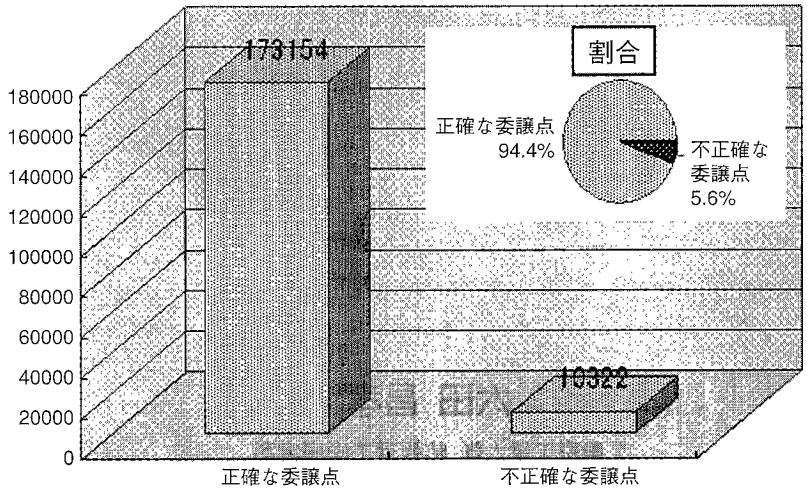


図-5　委譲の正確性に関する統計

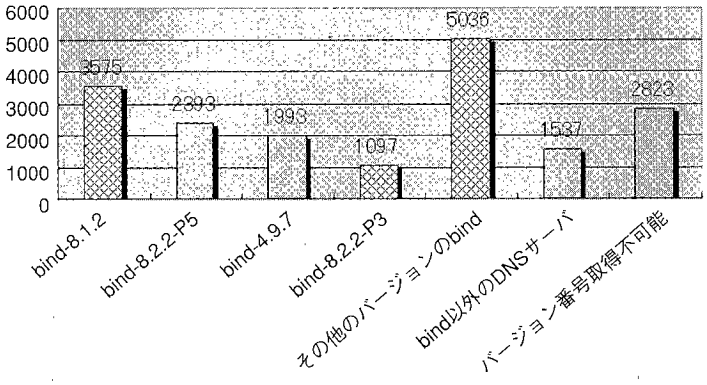


図-6　DNSサーバのバージョン番号に関する統計

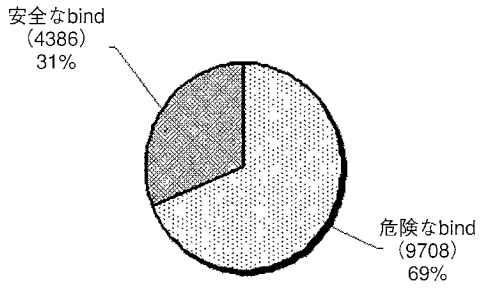


図-7　危険なbindと安全なbindの割合

入の基盤を整えることが，これからのDNSに課せられている急務の課題であるといえよう．

これからのインターネットは，計算機がつながるだけではなく，さまざまな機器が接続されると予想される．つまり，インターネットはそれら機器をつなぐインフラとして利用され，今まで以上の信頼性が求められるようになると考えられる．すると，DNSにもさらなる信頼性が要求され，セキュリティ向上が必須要件となるであろう．

現在のDNSにとって，セキュリティ新技術導入の第一歩は，新技術導入の基盤を整えることである．すなわち，前述した2つの前提条件を達成することである．そのためには，条件達成を援助するシステムが必要であり，本システムはその一端を担うことができると考える．たとえば，不正確な委譲点に関しては，本システムを利用すれば，不正確な委譲点となるゾーンと，その両DNSの管理者に関する情報を容易に抜き出すことができる．また，危険なDNSサーバの発見に関しても，本システムを用いれば，危険なDNSサーバとその管理者に関する情報を容易に抜き出すことができる．最後に，本システムと本調査に関して，的確なアドバイスと環境を与えてくれたBill Manning氏に感謝の意を表する．

参考文献
1) Eastlake, D.: Domain Name System Security Extensions, RFC2535, Internet Engineering Task Force (Mar. 1999).
2) Vixie, P., Gudmundsson, O., Eastlake, D. and Wellington, B.: Secret Key Transaction Authentication for DNS (TSIG), RFC2845, Internet Engineering Task Force (May 2000).
3) Eastlake, D.: 3rd, DNS Request and Transaction Signatures (SIG (0)s), RFC2931, Internet Engineering Task Force (Sep. 2000).
4) Eastlake, D.: 3rd, Secret Key Establishment for DNS (TKEY RR), RFC2930, Internet Engineering Task Force (Sep. 2000).
5) Williamson, S., Kosters, M., Blacka, D., Singh, J. and Zeilstra, K.: Referral Whois (RWhois) Protocol V1.5, RFC2167, Internet Engineering Task Force (June 1997).
6) CERT Advisory CA-1999-14 Multiple Vulnerabilities in BIND (http://www.cert.org/advisories/CA-1999-14.html), BIND Vulnerabilities (http://www.isc.org/products/BIND/bind-security-19991108.html).

(平成12年10月27日受付)